1-3-2019

Cyber Threat Report 03 January 2019

Patrick Bell
Army Cyber Institute

CYBER THREAT REPORT

January 3, 2019

Threat Actor Update

Iran's Charming Kitten group beats two-factor authentication

Cerfa Lab detected a phishing campaign against US Government officials, nuclear scientists, and others targeting Time-based One-time Password Codes

Hackers are posing as Chinese government for attacks

Brandon Helms of Rendition Infosecurity says increasingly prevalent because most hackers have access to the same publicly available tools that China favors.

Senate reports ongoing Russian social media influence effort

A report released by the Senate intelligence committee asserts Russian interference operations still exist on social media platforms.

US indicts two Chinese nationals over state-sponsored hacking

The Department of Justice alleges Chinese nationals were backed by China's Ministry of State Security in targeting banks, telecom companies, healthcare providers, NASA, and the US Navy.

Threat Target Update

European Union diplomatic communications network hacked

Hackers infiltrated the EU's diplomatic network for years, downloading thousands of cables concerning President Trump, Russia, China, and Iran's nuclear program.

NASA server hacked, exposing employee information

NASA claims there is no indication that any mission was impacted by the breach and has not revealed details as to how the server was breached or what group was behind it.

Hackers increasingly adept at stealing student data

The 2018 Education Cybersecurity Report shows that education ranks last of 17 industries in the US in terms of overall cybersecurity posture.
Related: San Diego school district data breach hits 500k students.

Federal agencies faced more than 35,000 cyber incidents in 2017

A Government Accountability Office report notes a 14 percent increase in cyber incidents from 2016 to 2017, and cites agencies with not effectively implementing the federal government's approach and strategy for securing information systems.

Malware targeting IoT devices grew 72% in Q3

According to McAfee Labs, malware attacks targeting IoT devices have grown 203% in the last year. The report also notes a rapid rise in cryptojacking and fileless malware.

ACI Update

- **General Joseph Votel, commander of U.S. Central Command, argues in Cyber Defense Review that the future of warfare demands more cyber authorities Read his article here.**
- **Download the full Fall 2018 Cyber Defense Review here.**
- **Read the Army.mil article on ACI's efforts to develop cyber leaders through the United States Military Academy's Cyber Policy Team.**
- **Relive the CYCON U.S. 2018 experience by exploring the video archives here.**

Tech Sector Update

News involving key players, products, and technologies

- **French data protection agency fines Uber €400k for a 2016 data breach**
- **Facebook admits giving partners access to messages**
- **FCC fines satellite startup Swarm Technologies $900k over unauthorized launch**
- **Amazon expands its fleet of Prime Air planes**
- **Dell Technologies, the largest privately held tech company, returns to public markets**

Regulation and Policy Update

News impacting the operational and regulatory environment

- **McKinsey article: Cybersecurity and the risk function**
- **President's National Infrastructure Advisory Council published study on Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation**
- **India's government to intercept, monitor, and decrypt citizens' computers**
- **FBI shuts down 15 DDoS-for-hire sites, charges three people for operating sites**
- **Cybersecurity views of Patrick Shanahn, new Acting SECDEF revealed in interview**
- **China plans new intellectual property law to protect foreign companies operating in China**

Contact Us
Army Cyber Institute at West Point
2101 New South Post Road
West Point, NY 10996
Phone: 845-938-3436
Web: https://cyber.army.mil
Email: threat.cyber@usma.edu